

Нараян Прасти

Блокчейн

Разработка приложений

Разработка децентрализованных приложений в реальном времени на платформе Ethereum



Packt

Building Blockchain Projects

Develop real-time practical DApps using Ethereum and JavaScript

Narayan Prusty



BIRMINGHAM - MUMBAI

Нараян Прасти

Блокчейн

Разработка приложений

Разработка децентрализованных
приложений в реальном времени
на платформе Ethereum

Санкт-Петербург
«БХВ-Петербург»

2018

УДК 004.75
ББК 32.973.26-018
П70

Прасти Н.

П70 Блокчейн. Разработка приложений: Пер. с англ. — СПб.: БХВ-Петербург, 2018. — 256 с.: ил.

ISBN 978-5-9775-3976-0

Рассказано о том, что такое децентрализованные приложения и как они работают. Рассмотрены принципы работы платформы Ethereum. Показано, как писать смарт-контракты и использовать интерактивную консоль Geth для размещения и передачи транзакций. Описана библиотека web3.js, ее импорт, подключение к Geth и использование в среде Node.js или на стороне клиента. Продемонстрировано, как создать сервис кошелька и управлять им, как компилировать смарт-контракты и развертывать их при помощи web3.js и EthereumJS. Описаны язык программирования Solidity и среда разработки Truffle. Приведено руководство по разработке собственного блокчейна и децентрализованных приложений корпоративного уровня.

*Для программистов, преподавателей и студентов,
а также специалистов отделов развития компаний и банков*

УДК 004.75
ББК 32.973.26-018

Группа подготовки издания:

| | |
|-----------------------|-----------------------------|
| Руководитель проекта | <i>Евгений Рыбаков</i> |
| Зав. редакцией | <i>Екатерина Капальгина</i> |
| Перевод с английского | <i>Валерия Яценкова</i> |
| Компьютерная верстка | <i>Ольги Сергиенко</i> |
| Оформление обложки | <i>Марины Дамбиевой</i> |

© Packt Publishing 2017. First published in the English language under the title 'Building Blockchain Projects - (9781787122147)'

© Packt Publishing 2017. Впервые опубликовано на английском языке под названием 'Building Blockchain Projects - (9781787122147)'

"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

ISBN 978-1-78712-214-7 (англ.)
ISBN 978-5-9775-3976-0 (рус.)

© Packt Publishing 2017
© Перевод на русский язык, оформление.
ООО "БХВ-Петербург", ООО "БХВ", 2018

Оглавление

| | |
|--|-----------|
| Предисловие к русскому изданию..... | 11 |
| Об авторе..... | 13 |
| О рецензентах..... | 15 |
| Издательство «Ракт»..... | 17 |
| Предисловие | 19 |
| О чем эта книга? | 19 |
| Что понадобится в дополнение к этой книге?..... | 20 |
| Для кого эта книга? | 20 |
| Обозначения..... | 20 |
| Обратная связь | 21 |
| Поддержка читателей..... | 22 |
| Скачивание исходных кодов программ | 22 |
| Цветные иллюстрации..... | 22 |
| Электронный архив файлов для русского издания..... | 23 |
| Исправления..... | 23 |
| Пиратство | 23 |
| Вопросы..... | 23 |
| Глава 1. Децентрализованные приложения..... | 25 |
| Что такое ДП? | 25 |
| Достоинства децентрализованных приложений..... | 27 |
| Недостатки децентрализованных приложений..... | 27 |
| Децентрализованная автономная организация | 27 |
| Личность пользователя в ДП..... | 28 |
| Учетные записи пользователей | 30 |
| Доступ к централизованным приложениям | 30 |
| Внутренняя валюта приложений..... | 31 |
| Недостатки внутренней валюты..... | 32 |

| | |
|--|-----------|
| Приложения с контролируемым доступом | 32 |
| Популярные приложения | 32 |
| Bitcoin | 32 |
| Что такое регистр? | 33 |
| Что такое блокчейн? | 33 |
| Легален ли биткойн? | 33 |
| Почему мы используем биткойн? | 34 |
| Ethereum | 34 |
| Hyperledger | 35 |
| IPFS | 35 |
| Как работает IPFS? | 36 |
| Filecoin | 36 |
| Namecoin | 37 |
| Домены в зоне <i>.bit</i> | 37 |
| Dash | 38 |
| Децентрализованное управление и бюджетирование | 39 |
| Децентрализованные услуги | 39 |
| BigChainDB | 40 |
| OpenBazaar | 40 |
| Ripple | 40 |
| Заключение | 43 |
| | |
| Глава 2. Принципы работы Ethereum | 44 |
| Знакомство с Ethereum | 44 |
| Учетная запись Ethereum | 45 |
| Транзакции | 45 |
| Консенсус | 46 |
| Метка времени | 48 |
| Число <i>nonce</i> | 48 |
| Время блока | 49 |
| Ветвление | 51 |
| Генезис | 52 |
| Деноминация эфира | 52 |
| Виртуальная машина Ethereum | 53 |
| Газ | 53 |
| Обнаружение узлов | 54 |
| Протоколы <i>Whisper</i> и <i>Swarm</i> | 55 |
| Geth | 55 |
| Установка Geth | 56 |
| OS X | 56 |
| Ubuntu | 56 |
| Windows | 56 |
| JSON-RPC и консоль JavaScript | 57 |
| Подкоманды и опции | 57 |
| Подключение к сети <i>mainnet</i> | 57 |
| Создание частной сети | 57 |
| Создание аккаунта | 58 |
| Майнинг | 58 |
| Быстрая синхронизация | 59 |

| | |
|--|-----------|
| Ethereum Wallet..... | 59 |
| Mist..... | 61 |
| Уязвимости Ethereum | 62 |
| Атака Сибиллы | 62 |
| Атака 51%..... | 62 |
| Обновление Serenity | 62 |
| Платежные каналы и каналы состояния | 63 |
| Протокол консенсуса Casper..... | 63 |
| Разделение данных | 64 |
| Заключение..... | 64 |
| Глава 3. Разработка смарт-контрактов | 65 |
| Файлы исходного кода Solidity | 65 |
| Структура смарт-контракта | 66 |
| Расположение данных | 67 |
| Что такое типы данных?..... | 68 |
| Массивы..... | 69 |
| Строки..... | 70 |
| Структуры | 71 |
| Перечисление | 72 |
| Сопоставление | 72 |
| Оператор <i>delete</i> | 73 |
| Преобразование элементарных типов..... | 74 |
| Ключевое слово <i>var</i> | 74 |
| Управляющие структуры | 75 |
| Оператор <i>new</i> и создание контракта | 76 |
| Исключения..... | 77 |
| Вызов внешних функций | 77 |
| Свойства контракта | 79 |
| Видимость | 79 |
| Модификаторы..... | 81 |
| Резервная функция..... | 83 |
| Наследование | 83 |
| Ключевое слово <i>super</i> | 85 |
| Абстрактные контракты..... | 86 |
| Библиотеки..... | 86 |
| Конструкция <i>using ... for</i> | 88 |
| Возврат нескольких значений | 89 |
| Импорт файлов исходных кодов Solidity | 89 |
| Глобальные переменные | 90 |
| Свойства блока и транзакции | 90 |
| Свойства, связанные с адресом | 91 |
| Переменные, связанные с контрактом | 91 |
| Единицы эфира | 91 |
| Доказательство наличия, целостности и принадлежности файла | 91 |
| Компиляция и развертывание контракта..... | 93 |
| Заключение..... | 96 |

| | |
|--|------------|
| Глава 4. Учимся работать с web3.js | 97 |
| Введение в web3.js..... | 97 |
| Импортирование web3.js..... | 98 |
| Подключение к узлу..... | 98 |
| Структура API..... | 99 |
| Библиотека BigNumber.js..... | 100 |
| Конвертация денежных единиц..... | 101 |
| Запрос цены газа, баланса и деталей транзакции..... | 101 |
| Отправка эфира..... | 103 |
| Работа с контрактами..... | 104 |
| Отслеживание событий контракта..... | 106 |
| Разработка клиентского приложения для контракта..... | 109 |
| Структура проекта..... | 110 |
| Разработка серверной части..... | 110 |
| Разработка клиентской части..... | 112 |
| Тестирование клиентской части..... | 116 |
| Заключение..... | 119 |
| | |
| Глава 5. Разработка сервиса кошелька..... | 120 |
| Различие между онлайн- и оффлайн-кошельками..... | 120 |
| Библиотеки hooked-web3-provider и ethereumjs-tx..... | 121 |
| Что такое HD-кошелек?..... | 124 |
| Введение в функции формирования ключа..... | 125 |
| Знакомство с LightWallet..... | 126 |
| Путь вывода HD-кошелька..... | 127 |
| Разработка сервиса кошелька..... | 127 |
| Предварительная подготовка..... | 127 |
| Структура проекта..... | 128 |
| Разработка серверной части..... | 128 |
| Разработка клиентской части..... | 129 |
| Тестирование..... | 136 |
| Заключение..... | 142 |
| | |
| Глава 6. Разработка платформы для смарт-контрактов..... | 143 |
| Вычисление <i>nonce</i> для транзакции..... | 144 |
| Знакомство с solcjs..... | 145 |
| Установка solcjs..... | 145 |
| API solcjs..... | 146 |
| Использование различных версий компилятора..... | 147 |
| Связывание библиотек..... | 148 |
| Обновление ABI..... | 149 |
| Разработка платформы для развертывания контрактов..... | 149 |
| Структура проекта..... | 150 |
| Разработка серверной части..... | 150 |
| Разработка клиентской части..... | 156 |
| Тестирование..... | 160 |
| Заключение..... | 161 |

| | |
|--|------------|
| Глава 7. Приложение для ставок на результат матча..... | 162 |
| Знакомство с Oraclize | 163 |
| Как работает Oraclize?..... | 163 |
| Источники данных..... | 163 |
| Доказательство подлинности..... | 164 |
| Стоимость услуг Oraclize..... | 166 |
| Основы работы с API Oraclize..... | 167 |
| Настройка типа и места хранения доказательства..... | 167 |
| Отправка запросов..... | 167 |
| Отложенные запросы..... | 168 |
| Расходование газа..... | 168 |
| Функции обратного вызова..... | 169 |
| Синтаксический разбор результатов..... | 170 |
| Получение цены запроса..... | 171 |
| Шифрование запросов..... | 171 |
| Расшифровка источника данных..... | 171 |
| IDE Oraclize..... | 172 |
| Работа со строками..... | 172 |
| Разработка контракта для ставок на спорт..... | 174 |
| Разработка приложения для ставок..... | 177 |
| Разработка структуры приложения..... | 178 |
| Разработка серверной части..... | 178 |
| Разработка клиентской части..... | 181 |
| Тестирование приложения..... | 189 |
| Заключение..... | 193 |
| | |
| Глава 8. Разработка смарт-контрактов уровня предприятия..... | 194 |
| Знакомство с <i>ethereumjs-testrpc</i> | 195 |
| Установка и использование <i>ethereumjs-testrpc</i> | 195 |
| Приложение командной строки <i>testrpc</i> | 195 |
| Использование <i>ethereumjs-testrpc</i> в качестве провайдера <i>web3</i> или HTTP-сервера..... | 197 |
| Доступные методы RPC..... | 198 |
| Что такое заголовки событий?..... | 199 |
| Знакомство с пакетом <i>truffle-contract</i> | 201 |
| Установка и импорт <i>truffle-contract</i> | 202 |
| Настройка тестового окружения..... | 203 |
| API <i>truffle-contract</i> | 203 |
| API абстракции контракта..... | 204 |
| Создание экземпляра контракта..... | 209 |
| API экземпляра контракта..... | 211 |
| Введение в Truffle..... | 212 |
| Установка Truffle..... | 212 |
| Инициализация Truffle..... | 212 |
| Компиляция контрактов..... | 214 |
| Файлы конфигурации..... | 214 |
| Развертывание контрактов..... | 215 |
| Файлы переноса..... | 216 |
| Написание кода переноса..... | 216 |

| | |
|---|------------|
| Юнит-тесты контрактов | 218 |
| Написание тестов на JavaScript | 219 |
| Написание тестов на Solidity | 221 |
| Как перевести валюту на тестовый контракт? | 224 |
| Запуск тестов..... | 224 |
| Управление пакетами | 225 |
| Управление пакетами через NPM | 225 |
| Управление пакетами через EthPM..... | 225 |
| Использование контрактов из пакета | 227 |
| Использование артефактов пакета в коде JavaScript | 227 |
| Доступ к адресам развернутых контрактов пакета в Solidity | 227 |
| Работа с консолью Truffle | 228 |
| Запуск внешних скриптов в контексте Truffle | 229 |
| Создание клиента в Truffle..... | 229 |
| Запуск внешних команд | 230 |
| Запуск пользовательских функций | 230 |
| Конструктор Truffle по умолчанию | 231 |
| Создание клиента..... | 233 |
| Сервер Truffle..... | 236 |
| Заключение..... | 238 |
| Глава 9. Разработка блокчейна для консорциума | 239 |
| Что такое блокчейн консорциума?..... | 240 |
| Что такое консенсус с доказательством полномочий?..... | 240 |
| Введение в Parity | 241 |
| Принципы работы Aura..... | 241 |
| Начинаем работу с Parity | 243 |
| Установка Rust | 243 |
| Скачивание, установка и запуск Parity | 244 |
| Создание частной сети | 244 |
| Создание аккаунтов..... | 244 |
| Создание файла спецификации | 244 |
| Запуск узлов..... | 248 |
| Подключение узлов | 249 |
| Полномочия и приватность..... | 249 |
| Заключение..... | 250 |
| Приложение. Описание электронного файлового архива..... | 251 |
| Предметный указатель..... | 253 |

Предисловие к русскому изданию

Уважаемые читатели!

Нам повезло жить в интересное время. На наших глазах и при нашем участии рождаются новые технологии, которые изменяют мир: блокчейн и децентрализованные приложения. Следует понимать, что сам по себе блокчейн ничего не значит. Революционные перемены зависят лишь от того, каким способом и в каких областях мы будем его применять. Книга, которую вы держите в руках, — один из редких образцов руководства по практическому применению технологии блокчейна.

Блокчейн вошел в нашу жизнь совсем недавно. Для этой технологии пока нет общепринятых законов и правил. Не удивительно, что возникают причудливые сочетания языков программирования и сред разработки, буквально в течение года успевают родиться и умереть новые протоколы и сервисы. Но уже настало время делиться опытом и говорить об устоявшихся подходах. Автор этой книги, Нараян Прасти, знает технологию блокчейна изнутри, потому что работает предметным экспертом по блокчейну в Национальном банке Арабских Эмиратов и последние пять лет занимается прикладной разработкой децентрализованных приложений.

Для продуктивной работы с материалом этой книги вам потребуются базовые знания и навыки в области программирования:

- ◆ основы объектно-ориентированного и функционального программирования. Следует знать, что такое объекты, классы, методы, конструкторы, функции. Полезно иметь навыки программирования на языке `C#`;
- ◆ навык программирования на языке JavaScript. Это обязательное условие для продуктивной работы с материалом книги. Программированию на JavaScript посвящено много хороших книг, и для вас не составит большого труда получить необходимые знания;
- ◆ умение работать со средой разработки и выполнения скриптов Node.js. Вы можете приступить к освоению Node.js параллельно с чтением двух первых глав этой книги.

При подготовке перевода мы тщательно проверили доступность всех ссылок, номера версий программ и обновили их по мере необходимости. В сносках указаны дополнительные ссылки и примечания, которые помогут в изучении материала. В сопровождающем книгу файловом архиве вы найдете исходные коды упражнений к главам книги, предоставленные издательством «Packt», и листинги исходных кодов примеров программ из текста.

Желаем успеха в практическом освоении новейшей технологии!

*Переводчик и научный редактор русского издания
Валерий Яценков*

Об авторе

Нараян Прасти (Narayan Prusty) — разработчик полного цикла, который в течение последних пяти лет специализируется на технологиях блокчейн и JavaScript. С присущей ему целеустремленностью он разрабатывал масштабируемые приложения для стартапов, правительства и предприятий в Индии, Сингапуре, США и ОАЭ.

Сегодня Нараян Прасти регулярно создает децентрализованные приложения на основе Ethereum, Bitcoin, Hyperledger, IPFS, Ripple и других протоколов. Он работает предметным экспертом по технологии блокчейн в Национальном банке Арабских Эмиратов, Дубаи.

Нараян Прасти уже написал две книги: *Learning ECMAScript 6* и *Modern JavaScript Applications*. Обе они опубликованы издательством «Packt»¹.

Он немедленно приступает к работе, если видит интересную захватывающую проблему. В возрасте 18 лет он разработал поисковый движок для файлов MP3 и до сегодняшнего дня создал много различных приложений, которыми пользуются люди по всей Земле. Его отличает уникальное умение разрабатывать масштабные проекты от начала до конца.

Сейчас Нараян видит свое предназначение в том, чтобы делать многие вещи проще, быстрее и дешевле при помощи технологии блокчейн. Он также ищет возможности предотвратить коррупцию, мошенничество и добивается открытости во всем мире при помощи блокчейн-приложений.

Вы можете больше узнать о авторе в его блоге: <http://qnimate.com> и найти его в сообществе LinkedIn: <https://www.linkedin.com/in/narayanprusty/>.

¹ На русском языке издана одна из этих книг: Введение в ECMAScript 6. М.: ДМК Пресс, 2016. — *Здесь и далее примечания переводчика, если не указано иное.*

О рецензентах

Имран Башир (Imran Bashir) получил степень магистра информационной безопасности в Королевском колледже Холлоуэй (Royal Holloway) при Лондонском университете и обладает опытом разработки программного обеспечения, управления инфраструктурой и ИТ-службами. Он входит в сообщества Института инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers, IEEE) и Британского компьютерного общества (British Computer Society, BSC). Имран имеет 16-летний опыт работы в государственном и финансовом секторах. Прежде чем перейти в индустрию финансовых услуг, он работал над крупными ИТ-проектами для государственного сектора и занимал разные технические должности в Лондоне — экономической столице Европы. Сейчас он вице-президент по технологиям в одном из инвестиционных банков Лондона.

Дэниел Крафт (Daniel Kraft) изучал математику и физику и получил степень доктора прикладной математики в Университете Граца, Австрия. Он подключился к разработке криптовалют в 2013-м году, был ведущим разработчиком и научным руководителем проектов Namecoin и Huntercoin в 2014-м году и опубликовал две исследовательских статьи в рецензируемых журналах. Дэниел работает инженером-программистом и является соучредителем компании Crypto Realities Ltd, которая создает многопользовательские игровые миры на основе технологии блокчейн.

Гуран Торвекар (Gaurang Torvekar) получил степень доктора по информационным системам в Сингапурском университете управления. Он соучредитель и технический директор компании Attores, расположенной в Сингапуре и обслуживающей смарт-контракты. Гуран имеет богатый опыт разработки приложений для Ethereum и Hyperledger. Он был докладчиком на нескольких конференциях по блокчейну, провел множество курсов по технологии блокчейн в Политехническом университете Сингапура и является ментором по блокчейну хакатона¹ Angelhack.

¹ Хакатон — форум разработчиков, во время которого специалисты из разных областей разработки программного обеспечения (программисты, дизайнеры, менеджеры) сообща работают над решением какой-либо проблемы. — *Ред.*

Издательство «Packt»

Знаете ли вы, что издательство «Packt» для каждой опубликованной книги предлагает электронные версии в форматах PDF и ePub? Купив печатную книгу, вы сможете на сайте www.packtpub.com получить ее электронное издание со скидкой для владельцев печатной версии¹. С вопросами обращайтесь по адресу; customercare@packtpub.com.

На сайте www.packtpub.com вы также можете найти множество бесплатных технических публикаций, подписаться на бесплатные рассылки и получать уникальные скидки и предложения.

Наиболее востребованные навыки разработки программного обеспечения вы можете получить на странице «Mapt» сайта издательства «Packt» по адресу: <https://www.packtpub.com/mapt>.

«Mapt» предоставляет полный доступ ко всем книгам и видеокурсам издательства «Packt», а также передовые инструменты, которые помогут вам в личном развитии и карьерном росте.

Что дает подписка?

- ◆ Полнотекстовый поиск по всем книгам издательства «Packt».
- ◆ Возможность ставить закладки, копировать и распечатывать фрагменты текста из книг.
- ◆ Печать книг по запросу и доступ к ним при помощи браузера.

¹ Разумеется, это относится только к покупателям исходного, английского издания книги. — *Ред.*

Предисловие

Блокчейн — это децентрализованный регистр, который содержит постоянно растущий список записей, защищенных от подделки и внесения изменений. Каждый пользователь может подключаться к сети, отправлять в нее новые транзакции, проверять транзакции и создавать новые блоки.

В этой книге рассказано, что такое блокчейн, как он обеспечивает целостность данных, и как создавать прикладные блокчейн-проекты на платформе Ethereum. На примере интересных реальных проектов вы узнаете, как писать смарт-контракты, которые выполняются именно так, как запрограммировано, без малейших шансов на мошенничество, цензуру или вмешательство третьей стороны, а также создавать приложения со сквозным шифрованием для блокчейна. Вы изучите такие основы, как криптография в криптовалютах, майнинг, смарт-контракты и язык программирования Solidity.

Блокчейн стал главным техническим новшеством биткойна, для которого служит публичным регистром транзакций.

О чем эта книга?

- ◆ **Глава 1. Децентрализованные приложения** — рассказывает о том, что такое децентрализованные приложения и как они работают.
- ◆ **Глава 2. Принципы работы Ethereum** — рассказывает о том, как работает Ethereum.
- ◆ **Глава 3. Разработка смарт-контрактов** — показывает, как писать смарт-контракты и использовать интерактивную консоль Geth для размещения и передачи транзакций.
- ◆ **Глава 4. Учимся работать с web3.js** — знакомит с библиотекой web3.js, рассказывает о том, как импортировать библиотеку, подключить ее к Geth и использовать в среде Node.js или на стороне клиента.

- ◆ **Глава 5. Разработка сервиса кошелька** — демонстрирует, как создать сервис кошелька и легко управлять Ethereum Wallets даже в режиме оффлайн. Мы воспользуемся для этого библиотекой LightWallet.
- ◆ **Глава 6. Разработка платформы для смарт-контрактов** — рассказывает о том, как компилировать смарт-контракты при помощи web3.js и развертывать их при помощи web3.js и EthereumJS.
- ◆ **Глава 7. Приложение для ставок на результат матча** — поясняет, как можно использовать сервис Ogaclize для выполнения HTTP-запросов из смарт-контрактов Ethereum, чтобы получить доступ к данным в Интернете. Мы также узнаем, как получать доступ к файлам, сохраненным в IPFS, научимся использовать строковую библиотеку и получим другие полезные навыки.
- ◆ **Глава 8. Разработка смарт-контрактов уровня предприятия** — подробно рассказывает, как использовать среду Truffle, которая значительно упрощает разработку децентрализованных приложений корпоративного уровня.
- ◆ **Глава 9. Разработка блокчейна для консорциума** — рассказывает о специфических особенностях разработки блокчейна для консорциумов.

Что понадобится в дополнение к этой книге?

Вам понадобится персональный компьютер с операционной системой Windows 7 SP1+, 8, 10 или Mac OS X 10.8+.

Для кого эта книга?

Эта книга предназначена для JavaScript-разработчиков, которые хотят создавать защищенные приложения для управления транзакциями и данными на основе блокчейна и Ethereum. Читатели, которые интересуются криптовалютами и доверенными хранилищами данных, найдут эту книгу чрезвычайно полезной.

Обозначения

В этой книге вы найдете несколько вариантов оформления текста, которые соответствуют различным типам информации. Продемонстрируем несколько стилей текста и поясним, что они обозначают.

Отдельные директивы программного кода, имена таблиц баз данных, имена файлов, расширения имен файлов, вводимые пользователем данные и строки Twitter обозначены шрифтом Courier. Например:

Затем запустите приложение при помощи команды `node app.js` внутри каталога `Final`.

Фрагменты кода выглядят так:

```
var solc = require("solc");
var input = "contract x { function g() {} }";
var output = solc.compile(input, 1); // 1 activates the optimizer
for (var contractName in output.contracts) {
  // logging code and ABI
  console.log(contractName + ": " +
    output.contracts[contractName].bytecode);
  console.log(contractName + "; " +
    JSON.parse(output.contracts[contractName].interface));
}
```

Текст, вводимый и выводимый в командной строке терминальных программ, обозначен **полужирным шрифтом Courier**, например:

```
# cp /usr/src/asterisk-addons/configs/cdr_mysql.conf.sample
  /etc/asterisk/cdr_mysql.conf
```

Надписи на кнопках и элементах меню программ обозначены **полужирным шрифтом**, например:

Снова выберите тот же самый файл и нажмите кнопку **Get Info**.



Таким значком обозначены важные примечания и комментарии.



Таким значком обозначены полезные советы и подсказки.

Обратная связь

Мы всегда благодарны читателям за отзывы. Расскажите нам, что вы думаете об этой книге, что вам понравилось или не понравилось. Отзывы читателей помогают нам готовить издания, которые действительно будут для вас полезны.

Для отправки отзыва общего плана достаточно написать нам по адресу электронной почты **feedback@packtpub.com**, указав название книги в теме письма.

Если вы хорошо разбираетесь в какой-либо теме и хотели бы написать книгу или стать соавтором, прочтите руководство для авторов: **www.packtpub.com/authors**.

Для читателей русского издания

Читатели русского издания могут оставлять свои отзывы на странице книги на сайте издательства «БХВ-Петербург» по адресу: **www.bhv.ru** или писать в издательство по адресу электронной почты: **mail@bhv.ru**.

Поддержка читателей

Поскольку вы стали правомочным обладателем книги издательства «Packt», мы поможем вам извлечь максимальную пользу из покупки.

Скачивание исходных кодов программ

Вы можете скачать исходные коды программ после регистрации на сайте **www.packtpub.com**. Независимо от места приобретения книги, зарегистрируйтесь по адресу: **https://www.packtpub.com/books/content/support** и получите файлы непосредственно на свою электронную почту¹.

Для скачивания исходных кодов с сайта издательства «Packt» выполните следующие шаги:

1. Войдите под своим именем или зарегистрируйтесь на сайте.
2. Наведите указатель мыши на закладку **SUPPORT** в верхней части сайта.
3. Щелкните на пункте **Code Download & Errata**.
4. Введите название книги или часть названия в поле **Search**.
5. Выберите нужную книгу в результатах поиска.
6. Выберите в раскрывающемся поле место покупки книги.
7. Щелкните на ссылке **Code Download**, которая появится ниже этого поля.

После скачивания воспользуйтесь одним из следующих архиваторов для извлечения файлов из архива:

- ◆ WinRAR или 7-ZIP — для Windows;
- ◆ Zipreg, iZip или UnRarX — для Mac;
- ◆ 7-Zip или PeaZip — для Linux.

Набор исходных кодов для этой книги также хранится на сайте GitHub по адресу: **https://github.com/PacktPublishing/Building-Blockchain-Projects**.

У издательства «Packt» есть и другие пакеты исходных кодов для обширного каталога их книг и видеокурсов. Они доступны по адресу:

https://github.com/PacktPublishing/

Цветные иллюстрации

Мы также предоставляем вам PDF-файл с цветными изображениями скриншотов и диаграмм, приведенных в этой книге. Цветные изображения помогут вам лучше понять, что имеется в виду. Вы можете скачать этот файл по ссылке:

https://www.packtpub.com/sites/default/files/downloads/BuildingBlockchainProjects_ColorImages.pdf

¹ Напомним, что эти предложения относятся только к покупателям исходного, английского издания книги. — *Ред.*

Электронный архив файлов для русского издания

Электронный архив с материалами к этой книге можно скачать с FTP-сервера издательства «БХВ-Петербург» по ссылке <ftp://ftp.bhv.ru/9785977539760.zip> или со страницы книги на сайте www.bhv.ru (см. *приложение*).

Исправления

Несмотря на все усилия и аккуратную работу над книгами, ошибки все-таки иногда проникают в текст. Если вы нашли ошибку в одной из наших книг — в тексте или в программе — мы будем признательны за сообщение о ней. Сделав это, вы убережете других читателей от огорчения и поможете нам улучшить следующее издание книги. Если вы нашли ошибку, пожалуйста, сообщите нам, зайдя на сайт по адресу: <http://www.packtpub.com/submit-errata>. Выберите вашу книгу, щелкните на ссылке: **Errata Submission Form** и введите текст своего замечания. После проверки ваша поправка будет одобрена и размещена на сайте в разделе для соответствующей книги.

Для просмотра ранее внесенных поправок перейдите по адресу: www.packtpub.com/books/content/support и введите название книги в поле поиска. Информация о правках размещена под заголовком **Errata**.

Пиратство

Вишение авторских материалов в Интернете стало общей проблемой для всех средств массовой информации. В издательстве «Packt» очень серьезно относятся к защите своих авторских прав и лицензий. Если вы обнаружили незаконную копию одного из наших изданий в любой форме, пожалуйста, незамедлительно сообщите нам физический адрес этого места или адрес веб-сайта, чтобы мы смогли принять меры.

Связаться с нами для отправки ссылки на нелегальные материалы можно по адресу электронной почты: copyright@packtpub.com.

Мы благодарны вам за помощь в защите наших авторов и наших усилий по разработке полезных материалов, которые мы создаем для вас.

Вопросы

Если у вас возникли затруднения с любыми аспектами использования этой книги, обращайтесь по адресу: questions@packtpub.com, и мы постараемся переадресовать ваш вопрос для наилучшего решения проблемы.

Читатели русского перевода книги могут обращаться с вопросами и пожеланиями по адресу издательства «БХВ-Петербург»: mail@bhv.ru.

1

Децентрализованные приложения

Почти все интернет-приложения, с которыми мы имели дело, являются *централизованными*, то есть серверы такого приложения принадлежат определенной компании или лицу. В течение длительного времени разработчики создавали централизованные приложения, а пользователи их применяли. Но у такого подхода есть проблемы, мешающие создавать определенные типы приложений. Централизованные приложения менее прозрачны, имеют конкретную точку отказа, не могут противостоять сетевой цензуре и т. д. На фоне этих проблем возникла новая технология разработки интернет-приложений, которые называются *децентрализованными приложениями* (Decentralized Applications, DApps).

В этой главе мы будем говорить о децентрализованных приложениях (ДП) и рассмотрим следующие темы:

- ◆ что такое ДП?
- ◆ в чем разница между децентрализованными, централизованными и распределенными приложениями?
- ◆ преимущества и недостатки централизованных и децентрализованных приложений;
- ◆ обзор структуры данных, алгоритмов и протоколов, применяемых в наиболее популярных ДП;
- ◆ некоторые популярные ДП, выстроенные поверх других децентрализованных приложений.

Что такое ДП?

Децентрализованные приложения — это особая разновидность интернет-приложений, основанных на одноранговой сети (peer-to-peer network) и имеющих открытый исходный код. Ни один узел сети не имеет полного контроля над ДП.